AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

initializing a pseudo-random number generator (PRNG);

obtaining local seeding information from a host;

securely obtaining additional seeding information from one or more remote ~~and independent~~ entropy servers; and

stirring the PRNG with the local seeding information and the additional seeding information.

2. (Currently Amended) The method of claim 1, wherein the initializing ~~a~~ of the PRNG comprises initializing ~~the~~ an internal state of the PRNG with a random value.

3. (Currently Amended) The method of claim 2, wherein the random value ~~is~~ comprises a seed.

4. (Currently Amended) The method of claim 1, wherein the securely obtaining of the seeding information from the one or more remote ~~and independent~~ entropy servers is repeated for redundant entropy servers.

5. (Currently Amended) The method of claim 1, wherein the one or more remote ~~and independent~~ entropy servers maintain random state pool to supply the host with the random value.

6. (Currently Amended) The method of claim 1, wherein the securely obtaining of the seeding information from the one or more remote ~~and independent~~ entropy servers ~~may include~~ includes using a privacy protocol.

7. (Original) The method of claim 6, wherein the privacy protocol comprises secure sockets layer (SSL) protocol.

8. (Original) The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. (Currently Amended) The method of claim 1, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.

Claims 10-16 (Cancelled)

17. (Currently Amended) An entropy enhancing system comprising:

a local system comprising a host, the local system further comprising a pseudo-random number generator (PRNG) to initialize the PRNG, to obtain local seeding information from the host, securely obtain additional seeding information from one or more remote entropy servers, and stirring the PRNG with the local seeding information and the additional seeding information; and

the one or more remote ~~independent~~ systems comprising the one or more entropy servers to securely provide the additional seeding information to the local system.

18. (Currently Amended) The entropy enhancing system of claim 17, wherein the local system ~~generates~~ to generate the local seeding information at the host.

19. (Currently Amended) The entropy enhancing system of claim 17, wherein the one or more remote ~~independent~~ systems ~~generate~~ to generate the remote seeding information at the one or more entropy servers.

20. (Currently Amended) The entropy enhancing system of claim 17, wherein the entropy servers ~~are~~ comprise one or more of the following:~~machines~~ hardware and software.

Claims 21-24 (Cancelled)

25. (New) A machine-readable medium having stored thereon data comprising sets of instructions which, when executed by a machine, cause the machine to:

initialize a pseudo-random number generator (PRNG);

obtain local seeding information from a host;

securely obtain additional seeding information from one or more remote entropy servers; and

stir the PRNG with the local seeding information and the additional seeding information.

26. (New) The machine-readable medium of claim 25, wherein the initializing of the PRNG comprises initializing an internal state of the PRNG with a random value.

27. (New) The machine-readable medium of claim 26, wherein the random value comprises a seed.

28. (New) The machine-readable medium of claim 25, wherein the securely obtaining of the seeding information from the one or more remote entropy servers is repeated for redundant entropy servers.

29. (New) The machine-readable medium of claim 25, wherein the one or more remote entropy servers maintain random state pool to supply the host with the random value.

30. (New) The machine-readable medium of claim 25, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.